

PROPOSED HSE GUIDELINES ON EMERGENCY
SHUTDOWN SYSTEMS

J. PEARSON

HEALTH & SAFETY EXECUTIVE, UK.

INTRODUCTION

Distributed control systems are becoming a standard form of control system in the oil, gas and process industries. These systems depend on computer technology for automatic control of the process conditions and offer advantages in terms of efficiency, high availability and in particular high levels of operator information. These advantages are exploited in a number of such industries in their search for increased production and hence profitability. These systems are however, complex inter-connected computer based systems and hence are difficult to analyse in terms of their reliability, failure modes and hence the effect of possible failure of the control system on plant safety. In such circumstances there are advantages from a safety view point in having a dedicated independent protection system or emergency shut down (ESD) system to take action to achieve a safe plant condition in the event of plant or equipment failure or indeed control system failure.

This protection has traditionally been implemented using custom designed and built relay systems or more recently solid state electronic modular systems hardwired to plant sensors and valves. As the size of these systems increase with plant complexity; and hence the number of inputs and outputs of the system, the advantages of using programmable electronic systems increases. At present there are no National standards specifically for Emergency Shut Down systems and so HSE propose to publish Guidelines on this subject in close cooperation and after full consultation with interested parties. The proposed HSE document will complement the E.E.M.U.A. Publication "Safety Related Instrument Systems for the Process Industries" to be published later this year.

PROTECTION SYSTEMS

The advantages of having a separate independent protection system are:-

- reduced possibility of common cause failures.
- reduced complexity.
- simplified safety and reliability analysis.
- flexibility for modifications to control systems without adverse safety effects.

APPLICATIONS

Emergency shutdown (ESD) systems can be applied to any hazardous plant which has a safe state to which the plant can be directed when things go wrong for any reason. ESD systems are commonly used in process plants handling flammable or toxic chemicals and

which have the potential for major hazard accidents. The complex nature of process plants requires that particular actions are taken in a particular set of circumstances to shut down the plant in order to make it safe.

In order to satisfy the requirement that a major hazard plant is "safe so far as is reasonably practicable" the ESD systems should be engineered to very high levels of integrity and availability.

From the financial considerations the ESD system needs to give high degree of freedom from spurious trips coupled with the capability for on-line maintenance and repair in order to reduce to a minimum the loss of production caused by equipment outages. These requirements along with the ever increasing demand for information both locally to the system and in remote control rooms are giving a strong incentive for companies to choose to take advantage of ESD systems based on programmable electronics.

ADVANTAGES OF PROGRAMMABLE ELECTRONIC SYSTEMS

There are several major advantages of programmable electronic systems (PES) when used for ESD systems:-

- self checking capabilities.
- full automatic testing.
- on-line monitoring of input and output circuits and devices.
- communications capability.
- access control for modifications.
- self-diagnostics.
- logging of tests and over-ride.
- high resolution event logging to aid post-incident investigations.
- self generating "as fitted" programme documentation (print-out of actualuser programme).

The HSE recognise these as potential advantages for safety but recommend that emergency shutdown systems irrespective of the technology on which they are based should be subject to a safety integrity assessment.

HSE GUIDELINES

HSE propose to publish a guidelines document specifically aimed at ESD systems including programmable electronic systems.

The guidelines will be in 3 parts

- Part I Introduction and Background.
With examples of ESD applications.

Part II Design and Assessment of ESD Systems.

Part III Qualitative Assessment Checklists and Commentary.

The guidelines will consider the whole life cycle of the ESD system and emphasis will be placed on providing practical advice on how to apply PES 2 to ESD systems.

The assessment of safety integrity of an ESD system needs to include the three aspects of:

- Configuration
- Quality
- Reliability

The first step in assessing any such safety related system is to identify and analyse the potential hazards of the application or installation. In installations presenting major accident hazards for example oil refineries, or chemical plants processing highly toxic or flammable gases and liquids there is need to employ several levels of safety systems. In most plants of this type the hierarchy of safety features is well established. A typical example would be:-

- integrity of containment systems.
- self acting pressure relief devices or systems.
- emergency shutdown systems.
- operator alarms.
- automatic process control system.

This hierarchy is referred to in the HSE guidelines as the "total configuration of systems" and there may be 2 or 3 levels of system which are referred to as the "safety related systems". In defining which systems are safety related the judgement has to be made on whether the mechanical integrity of the plant along with pressure relief systems is adequate in all circumstances or whether other protection systems are required to protect the plant fully. If the plant is not considered safe without a fully operational emergency shutdown system then that is clearly a safety related system. The requirements of the HSE guidelines for a systematic assessment apply equally well in these circumstances to all technologies as well as programmable electronic systems and the fundamental criterion is that the plant should be "safe so far as is reasonably practicable" (Health and Safety at Work Act Section 2).

In major hazard installations the requirement is therefore for high levels of safety integrity including hardware reliability, high quality procedures in design manufacture testing and installation and high quality software design and implementation. In terms of emergency shutdown systems it is considered reasonably practicable therefore to employ the best designs in terms of fault tolerance and fault avoidance techniques all within a total quality approach.

CONFIGURATION

There are many possible configurations of shutdown systems. For example redundancy of

inputs, redundancy of processing units or logic, redundancy of output circuits or any combination of these can be used to give the desired level of hardware reliability. It should be noted here that redundancy is not a precaution against failures of the system such as fundamental errors or environmental effects which will always affect all components in a redundancy system given the same circumstances.

A typical emergency shutdown system may have single inputs from single sensors for non-critical parameters, 'one out of two' inputs for safety critical process parameters or 'two out of three' inputs where high safety integrity combined with high availability is required.

Logic processing for the functional requirements can be carried out by solid state logic, relay logic or programmable systems based on programmable logic controllers. Outputs are usually solenoid valves acting on process trip valves or on safety critical applications by duplicate solenoid valves operating on duplicate trip valves in series.

The use of programmable logic controllers based on a dual redundancy configuration has been adopted by a number of manufacturers of emergency shutdown systems. The levels of redundancy adopted should take account of the relative reliabilities of components in the system from input to output and for optimum hardware reliability a balance has to be found between level of redundancy and simplicity as increased complexity leads to increased maintenance and operator errors and hence sets a limit on the level of reliability achievable.

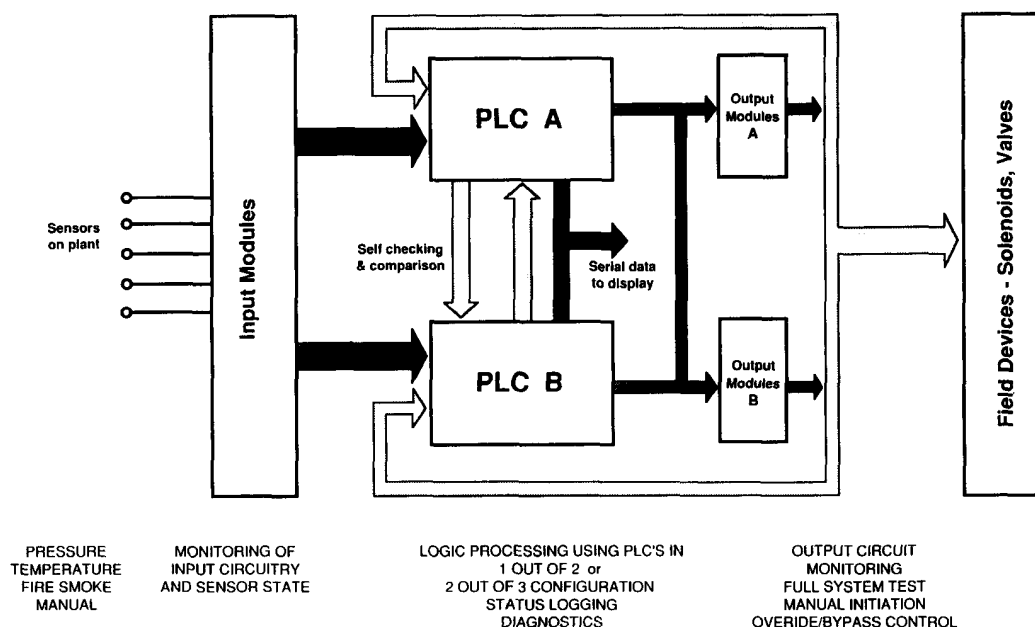
A typical modern Programmable ESD system is shown in Fig. 1.

The configuration of the ESD system components can be designed such that an optimum level of reliability of the hardware is achieved by using redundancy and self checking features. The optimum hardware reliability and configuration using computer technology could be achieved by adopting:-

- high reliability components.
- dual processing and self checking.
- one out of two configuration.
- two out of three inputs for optimum availability without compromising safety.
- on line maintenance capability.
- output devices to suit the process needs (duplication of trip valves, and diversity of solenoid valves if appropriate).
- on line monitoring of inputs up to the sensor contacts.
- monitoring of output actuator and wiring.
- full self test.
- communications to Distributed Control System.

SINTEF, the Norwegian Institute of Technology Research Foundation are researching into the comparative reliabilities of a variety of different configurations of ESD systems on behalf of a group of major offshore oil companies. The reports to date give very useful information (Ref 3.).

Fig 1 A TYPICAL PROGRAMMABLE ESD SYSTEM



SYSTEMATIC INTEGRITY (OVERALL QUALITY)

The level of reliability and configuration given above however, does not protect against errors in the specification, misunderstandings or incorrect assumptions about the plant state, or failure to fully consider the effect of modifications on plant safety, all of which can totally invalidate the ESD system. This fact is well demonstrated by a serious explosion and fire at a major refinery which occurred due to concurrent failure of control system, alarm system and shut-down systems along with inadequate pressure relief. This accident caused loss of life and major financial loss.

Accident records demonstrate that this type of failure or systematic failure, accounts for the majority of failures of control and protection systems. The HSE recommendation in PES2 is for a high commitment to quality at all phases of the life cycle of ESD systems from concept stage through specification, design and manufacture to operation and maintenance. The proposed guidelines will give advice on these qualitative aspects of safety integrity by reference to sound engineering principles and quality assurance measures. The guidelines

will include general recommendations by reference to checklists comprising questions and answers and commentary on good practice.

CONCLUSION

Modern programmable systems offer extremely high levels of reliability but require an appropriate level of attention to detail during design, manufacture, commissioning and operation to ensure high systematic integrity. The reliability of sensors and actuators on which ESD systems depend entirely for safe plant operation will continue to be a limiting factor to the overall level of reliability achievable. Modern state of the art technology and techniques however such as addressable sensors with self calibrating capability, and valve actuators with position monitoring can be applied to increase overall reliability. The cost of the features and the degree of redundancy throughout the system and hence further complexity needs to be balanced against the hazards and potential consequences of system failure.

The ESD Guidelines document should help both manufacturers and users to make these decisions and so take advantage of modern technology whilst improving overall plant safety.

REFERENCES

1. "Programmable Electronic Systems in safety related applications";
Part 1 "An Introductory guide"
Part 2 "General Technical Guidelines"
Health & Safety Executive, HMSO 1987.
2. Safety Related Instrument Systems for the Process Industries (including Programmable Systems) Publication No 160. The Engineering Equipment and Materials Users Association 1989.
3. Configuration of Computer-Based Process Safety Systems. Report No STF4P A87012. SINTEF, The Foundation for Scientific and Industrial Research at the Norwegian Institute of Technology 1987.

© Crown Copyright